FORTRA

GUIDE

What Is Data Classification And What Can It Do For My Business?

Including

- Paper-based classification policies
- Automated and user-driven data classification
- How to prepare for a data classification project
- The peripheral benefits of involving the user in security

Indroduction

Data classification is an approach to identifying, protecting and managing information which has rapidly become best practice. Implemented as part of a layered security strategy, it enables an enterprise to defend itself against a variety of threats - from aggressive outsiders to untrained or well-meaning insiders - while unlocking the full potential of its data to drive innovation and productivity.

At its simplest level, data classification is "the process of organising data into categories for its most effective and efficient use". From a security perspective classification involves the categorisation and labelling of data according to its level of sensitivity or value to an organisation – for instance as commercial in confidence, internal only or public. The approach switches the focus of data security from building 'walls' around networks, databases, applications or devices – increasingly ineffective, as 95% of breaches are caused by human error (your users are on the inside of any "wall") – to the data itself.

The first step is to establish a policy as to what labels or classifications should be added to which files or emails. The company can then decide how to communicate this to employees and make a decision on how to implement the policy. Some organisations decide to adopt a manual only labelling policy however, there are more advanced data classification techniques that utilise software toolsets which attach labels to email messages, documents and files. In addition to a visual marking that lets people know how the data should be handled, the label is embedded into the file properties as metadata, allowing the data to be accessed or used only in accordance with the rules that correspond with the data's classification. This means that the protection travels with the data, wherever it is sent or stored.

Each of the three techniques – **paper-based classification, automated classification** and **user-driven (or user-applied) classification** – has its own benefits and pitfalls.

Paper-Based Classification Policy

A corporate data classification policy will set out how employees are required to treat the different types of data they handle, aligned with the organisation's overall data security policy and strategy. A well-written policy will enable users to make fast and intuitive decisions about the value of a piece of information, and what the appropriate handling rules are for example who can access the data and should a rights management template be invoked. The challenge, without any supporting technology, is ensuring that everyone is aware of the policy and implements it correctly

Automated Classification Policy

This technique bypasses the users' involvement, enforcing a classification policy to be consistently applied across all touchpoints, without the need for major communication and education programmes.

Classifications are applied by solutions that use software algorithms based on keywords or phrases in the content to analyse and classify it. This approach comes into its own where certain types of data are created with no user involvement – for example reports generated by ERP systems or where the data includes specific personal information which is easily identified such as credit card details. However, automated solutions do not understand context and are therefore susceptible to inaccuracies, giving false positive results that can frustrate users and impede business processes, as well as false negative errors that expose organisations to sensitive data loss.

User-Driven Classification Policy

The data classification process can be completely automated, but it is most effective when the user is placed in the driving seat.

The user-driven classification technique makes employees themselves responsible for deciding which label is appropriate, and attaching it using a software tool at the point of creating, editing, sending or saving. The advantage of involving the user in the process is that their insight into the context, business value and sensitivity of a piece of data enables them to make informed and accurate decisions about which label to apply. User-driven classification is an additional security layer often used to complement automated classification.

Involving users in classification also leads to other organisational benefits including increased security awareness, an improved culture and the ability to monitor user behaviour which aids reporting and provides the ability to demonstrate compliance. Furthermore, managers can use this behavioural data to identify a possible insider threat, and address any concerns by providing additional guidance to users as appropriate, for example through additional training or by tightening up policy.

Involving The User In Security Has Peripheral Benefits

Taking a user-driven classification solution approach allows controls, rules and policies to be consistently enforced throughout the organisation. It also delivers additional benefits:

Use Metadata To Protect Critical Data Through Its Journey

As well as shielding the business from hacker activity, the classification of data guards against accidental data loss from within the organisation. The metadata tag directs the actions of other downstream enterprise security and data management solutions – triggering rules so that, for example, an email gateway will automatically encrypt any file marked Confidential, while a data loss prevention (DLP) solution will block employees from uploading the file to a cloud file share service.

The approach also enhances the effectiveness of security incident and event monitoring (SIEM) tools, allowing unusual and potentially risky user behaviour to be detected early on. If a user is consistently downgrading files from Confidential to Public, for example, or is copying sensitive documents to a storage device, this will be flagged up. The issue can then be addressed through training, disciplinary procedures or strengthening of policy.

Meet Regulatory Requirements And Demonstrate Compliance

Regulatory violations can lead to crippling fines, huge post event clean-up costs in the case of a breach and even criminal charges. Classifying data makes it easier for a business to meet the data governance requirements of the **Data Protection Act**, the **European General Data Protection Regulation (GDPR)**, the **Sarbanes-Oxley Act**, **HIPAA** and **ITAR**, for instance.

How To Prepare For A Data Classification Project: 3 Key Steps

1. Evaluate Your Data

- What types of data do you have?
- Where does it reside (e.g databases, cloud storage, employees' email folders)?
- How much of that data is regulated?
- What policies and controls are in place to protect the data?
- Who has access to the data?

2. Define It's Value

- What would the impact or risk be to the organisation if the data was compromised (e.g. erosion of competitive advantage due to loss of IP, leakage of customers' personal details)?

3. Scope Out Your Policy

- Who should have access to each type of data?
- How many classification categories will you have? Keep them minimal.
- What will they cover? Define the labels clearly, using a commonly understood language.
- What classification approach will you follow – automated or user-driven?
- Which technology solution will you adopt? This could range from a simple internally-developed tool to a comprehensive third party software package.
- How will you communicate the policy, and train people to use the selected solution?

The embedding of the classification label as metadata within files allows an enterprise to audit exactly who is accessing sensitive information, and keep a detailed trail of any policy violations or unusual behaviour. In addition to enabling potential breaches to be rapidly identified and addressed, this can be used to prove to the board, industry bodies and regulators that information is being appropriately controlled and documented.

Drive A Culture Of Security

The implementation of a user-driven classification process helps to build a culture of security awareness across the organisation. It puts the onus of protecting data on everyone who handles it, ensuring that all employees understand the value of the information they work with on a daily basis, and know how to treat it.

Data classification tools that incorporate the labelling of messages, documents and files into employees' routine work processes, meanwhile, will help to drive the right behaviours.

Facilitate Safer Collaboration

Data classification provides organisations with a means of building security into the corporate culture in a way that fosters, rather than inhibits, the power employees have to work in more productive and agile ways. Because the protection travels with the individual pieces of data on their 'journey', systems and databases can be safely integrated, and ideas and information shared freely between people, without exposing data to unauthorised access or use.

Manage And Use Data More Effectively

Before you can make full use of your data you need to know what you've got and where it is. The huge volume of unstructured data that organisations hold – such as email messages, Word documents, PowerPoint decks, Excel files, images and videos – make this increasingly difficult to get a grip on. Classifying data makes it possible to establish exactly what is there, where it is stored, and how valuable it is. It also helps the business to identify what can be archived or deleted, and so avoid the high protection, storage and retention costs associated with hoarding vast amounts of data.

Global brands trust us to protect their sensitive data:

pwc

Ministry of Defence

Honeywell

PRUDENTIAL

AMGEN

SOCIETE GENERALE

Allianz

Raytheon

More Information

For more information about how you can implement a data classification solution as part of your data protection strategy, please **contact us**

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.